



蓝海卓越 NSWMP 管理协议

协议设计：李杰

技术审核：刘岗

版本：V0.3

版权所有：www.natshell.com

修订记录

日期	版本	修订说明	修订人
2014/12/25	V0.1	初稿	李杰
2015/1/13	V0.2	修复更新	李杰
2015/2/2	V0.3	修复更新	李杰

目录

一、	前言.....	- 1 -
二、	AP 状态机.....	- 2 -
2.1	综述.....	- 2 -
2.2	AP 状态详解.....	- 2 -
2.2.1	初始化状态.....	- 2 -
2.2.2	发现状态.....	- 2 -
2.2.3	沉默状态.....	- 3 -
2.2.4	加入状态.....	- 3 -
2.2.5	固件更新状态.....	- 3 -
2.2.6	运行状态.....	- 3 -
2.2.7	等待状态.....	- 4 -
2.2.8	会话恢复状态.....	- 4 -

2.3 AP 状态转移图.....	- 4 -
三、AC 状态机.....	- 6 -
3.1 综述.....	- 6 -
3.2 状态详解.....	- 6 -
3.2.1 初始化状态.....	- 6 -
3.2.2 发现状态.....	- 6 -
3.2.3 加入状态.....	- 6 -
3.2.4 更新固件状态.....	- 7 -
3.2.5 运行状态.....	- 7 -
3.2.6 等待状态.....	- 7 -
3.2.7 恢复会话状态.....	- 7 -
3.3 状态转移图	- 8 -
四、协议基本格式.....	- 9 -
4.1 协议头.....	- 9 -
4.2 协议具体格式定义	- 10 -
4.2.1 密钥请求 (Secret Key Request)	- 10 -
4.2.2 密钥回复 (Secret Key Response)	- 10 -
4.2.3 发现请求 (Discover Request)	- 10 -
4.2.4 发现回应 (Discover Response)	- 10 -
4.2.5 加入请求 (Join Request)	- 11 -
4.2.6 加入回应 (Join Response)	- 11 -

4.2.7 回声请求 (Echo Request)	- 11 -
4.2.8 回声响应 (Echo Response)	- 12 -
4.2.9 重启 AP 请求 (Reboot Request)	- 12 -
4.2.10 重启 AP 回复 (Reboot Response)	- 12 -
4.2.11 AP 重连请求 (Reconnect Request)	- 12 -
4.2.12 AP 重连回复 (Reconnect Response)	- 12 -
4.2.13 AP 恢复会话请求 (Recover Request)	- 13 -
4.2.14 AP 恢复会话回复 (Recover Response)	- 13 -
4.2.15 固件完成 (Image Data Response)	- 13 -
4.2.16 新用户请求 (New User Request)	- 13 -
4.2.17 新用户回复 (New User Response)	- 14 -
4.2.18 用户授权请求 (User Accredited Request)	- 14 -
4.2.19 用户授权回复 (User Accredited Response)	- 14 -
4.2.20 用户下线请求 (User Left Request)	- 14 -
4.2.21 用户下线回复 (User Left Response)	- 15 -
4.2.22 强制用户下线请求 (User Drop Request)	- 15 -
4.2.23 强制用户下线回复 (User Drop Response)	- 15 -
4.2.24 用户计费请求 (User Account Request)	- 15 -
4.2.25 用户计费回复 (User Account Response)	- 16 -
五、消息属性.....	- 17 -
5.1 SECRET KEY	- 17 -
5.2 AP BOARD DATA	- 18 -

5.3 AC IPv4 地址 (AC IPv4 ADDRESS)	- 18 -
5.4 RESULT CODE.....	- 19 -
5.5 ECHO TIME	- 19 -
5.6 IDLE TIME.....	- 20 -
5.7 WiFi CONFIGURATION	- 20 -
5.8 PORTAL CONFIGURATION	- 22 -
5.9 FREE IP	- 22 -
5.10 IMAGE IDENTIFIER.....	- 23 -
5.11 ACCOUNT TIME	- 23 -
5.12 FREE HOST	- 24 -
5.13 USER INFORMATION	- 24 -
5.14 USER QUOTA.....	- 25 -
5.15 USER STATISTICS.....	- 26 -
六、AP 固件升级	- 28 -
七、消息加密.....	- 29 -
八、附录.....	- 30 -
8.1 802.11 无线类型代码定义	- 30 -
8.2 PORTAL 协议代码定义.....	- 30 -
8.3 无线加密代码定义	- 31 -
8.4 无线加密算法代码定义	- 31 -

本次修订记录

- 1、增加通信加密部分
- 2、修改了 Free IP 属性格式
- 3、增加上报计费周期
- 4、增加 Free URL 属性
- 5、修改密钥协商阶段 AC 回复 AP 是否使用该密钥消息为加密消息
- 6、修改 WiFi Configuration 属性内容，使其支持多 SSID
- 7、添加附录，定义相关代码值

一、前言

蓝海卓越基于自身对无线认证市场需求的发掘，以及对市场上主流 Portal 协议的深入了解，推出了基于 CMCC/华为 Portal 协议的产品。但在各种 Portal 和无线认证项目的交付中，蓝海卓越发现基于 CMCC 和华为 Portal 协议的无线认证网络存在业务功能缺陷以及各品牌产品之间兼容性的问题，很大程度上影响了项目的实施和交付。

在积累了多达上百个 Portal 项目实施案例的经验后，充分把握无线认证市场需求，蓝海卓越于近期推出自有的 NSWMP 管理协议。该协议完全由蓝海卓越自行设计架构，在满足目前市场需求和未来技术发展方向的基础上，避免华为协议在业务功能上的缺陷和 CMCC 协议存在的方言性，使之可以成为众多 AC/AP 厂家、无线广告运营商、广告路由厂家及其他网络设备厂家皆可方便有效采用的无线认证协议标准。

二、AP 状态机

2.1 综述

为了简化与适应 WIFI 新的业务要求，现将 AP 的状态分为初始化状态（INIT）、发现状态（Discovery）、沉默状态（Sulking）、加入状态（Join）、固件更新状态（Image Update）、运行状态（Run）、等待状态（Wait）、会话回复状态（Recover）八个状态。

2.2 AP 状态详解

2.2.1 初始化状态

AP 在初始化状态下读取配置的 AC 地址，如果没有配置 AC 地址，则退出程序；解析到 AC 的地址且网络畅通，随机等待一段时间(3 至 10 秒)，跳转状态到发现状态。

2.2.2 发现状态

该状态下 AP 向 AC 发送发现请求（Discovery Request），并设置等待回复定时器(超时时间 3 秒)以等待 AC 的发现响应（Discovery Response）。该状态下可能出现一下两种情况：

- （1）无发现响应（Discovery Response），则状态切换到沉默状态（Sulking）；
- （2）收到发现响应（Discovery Response），则状态切换到加入状态（Join）。

2.2.3 沉默状态

本状态下等待一定的时间(随机等待一段时间, 时间范围为 10 到 20 秒), 再次切换到发现状态。在沉默状态, 忽略收到的一切消息。

2.2.4 加入状态

AP 向 AC 发送加入请求 (Join Request), 并设置等待定时器(超时时间 1 秒), 等待 AC 的加入响应 (Join Response)。

(1) 如果定时器超时, 则切换状态到沉默状态;

(2) 在加入响应消息中, a)如果有固件更新内容, 则切换状态到固件更新状态 (Image Update); b) 没有固件更新内容, 且加入响应消息中指示允许加入, 并包含相关配置参数, 则跳转状态到运行状态 (Run); c) 加入响应消息中指示加入失败, 则跳转状态到沉默状态。

2.2.5 固件更新状态

本状态下, AP 从 AC 获取固件, 完成获取后, 自动更新固件, 完成后自动重启。

AP 从 AC 获得固件文件名字, 固件文件名后带随机码字符串, 该随机码字符串长度为 36 字节, 在 AP 获取固件时, 需要提交该随机码字符串以验证。

2.2.6 运行状态

本状态下, AP 主动向 AC 发送心跳检测消息, 并设置定时器(该定时器超时时间为 ECHO Time), 等待心跳回复。如果在超时时间内, 收到心跳回复, 维持

当前状态；超时时间内没有收到心跳回复(失败阈值为 3 次)，则切换状态到等待状态 (Wait)。

2.2.7 等待状态

本状态下，AP 将不再为新的用户提供服务，保持已有的用户会话。在该状态下向每隔 5 秒向 AC 发送一次重连请求，如果收到重连回复，则跳转状态到会话恢复状态；如果一直未收到回复(向 AC 发送了 60 次重连请求)，则 AP 重启。

2.2.8 会话恢复状态

AP 在该状态下向 AC 上报当前的运行状态，包括用户、运行配置参数等信息，上报成功则跳转状态到运行状态，(重试次数为 2 次，重试间隔为 3 秒)不成功则 AP 重启。

2.3 AP 状态转移图

	INIT (S0)	DISCV (S1)	SULK (S2)	JOIN (S3)	IMAGE (S4)	RUN (S5)	WAIT (S6)	RECOV (S7)
INIT(E0)	A0/S1							
DISCV REP(E1)		A1/S3						
DISCV Timer(E2)		A2/S2						
SULK Timer(E3)			A3/S1					
JOIN REP 无固件更新(E4)				A4/S5				
JOIN REP 固件更新(E5)				A5/S4				
JOIN Timer(E6)				A6/S2				
Update Done(E7)					A7/S0			
ECHO REQ(E8)						A8/S5		
ECHO Timer (E9)						A9/S6		
RECONN							A10/S7	

REP(E10)								
WAIT Timer(E11)							A11/S0	
RECOV OK(E12)								A12/S5
RECOV Error(E13)								A13/S0
RECOV Timer								A14/S0

事件说明：

E0 ： 初始化状态在初始化环境完成后，随机等待一段时间，E0 为该等待时间超时而发送发现请求(Discovery Request)；

E1 ： AP 向 AC 发起发现请求 (Discovery Request) 后，接收到发现响应 (Discovery Response) 消息；

E2 ：接收发现请求 (Discovery Response) 消息超时；

E3 ：沉默状态超时时间；

E4 ：加入响应消息中无固件更新要求；

E5 ：加入响应消息中有固件更新要求；

E6 ：加入请求定时器，接收加入响应消息超时；

E7 ：固件更新完成；

E8 ：AP 向 AC 发送心跳检测请求，接收到心跳回复；

E9 ：接收心跳回复消息超时；

E10 ：AP 向 AC 发起 Reconnect 请求，且重新链接成功；

E11 ：等待状态中重新链接未成功，等待时间超时；

E12 ：恢复会话状态成功；

E13 ：恢复会话状态出错。

三、AC 状态机

3.1 综述

AC 状态分为初始化状态(INIT)、发现状态(Discovery)、加入状态(Join)、更新固件状态(Image Update)、运行状态(Run)、等待状态(Wait)、会话恢复状态(Recover)七个状态。

3.2 状态详解

3.2.1 初始化状态

AC 在该状态下，等待接收 AP 的发现请求。当接收到 AP 发现消息时，跳转状态到发现状态。

3.2.2 发现状态

本状态下处理 AP 的发现请求，返回发现响应消息(Discovery Response)，切换状态到加入状态(JOIN)，开启等待加入定时器(超时时间为 2 秒)。

3.2.3 加入状态

(1) 接收到 AP 加入请求(Join Request)消息，关闭定时器，AC 根据 AP 提供的信息下发固件更新指示或者下发运行配置参数。如果下发固件更新指示，跳转状态到固件更新状态(IMAGE)，并开启定时器(超时时间为 300 秒)；如果下发运行配置参数，跳转状态到运行状态(RUN)，开启心跳定时器。

(2) 定时器超时未接收到加入请求消息，跳转状态到初始化状态。

3.2.4 更新固件状态

(1) 接收到固件更新请求, 关闭定时器, 返回固件消息。跳转状态到初始化状态。

(2) 未接收到固件更新请求, 定时器超时, 跳转状态到初始化状态。

3.2.5 运行状态

(1) 接收到心跳请求, 关闭定时器, 返回心跳回复, 开启心跳定时器(超时时间为 ECHO TIME);

(2) 心跳定时器超时, 未接收到心跳请求, 切换状态到等待状态, 开启等待定时器(超时时间为 60 秒)。

3.2.6 等待状态

在该状态下, 等待接收 AP 的重连请求, 如果定时器超时未接收到重连请求, 跳转状态到初始化状态。接收到重连请求, 回复重连响应, 跳转状态到恢复会话状态, 开启恢复会话定时器(超时时间为 5 秒)。

3.2.7 恢复会话状态

在定时器时间内, 接收到恢复会话请求, 关闭定时器, 恢复 AP 的会话信息。回复恢复状态响应, 如果恢复成功, 跳转状态到运行状态, 恢复失败跳转状态到初始化状态。

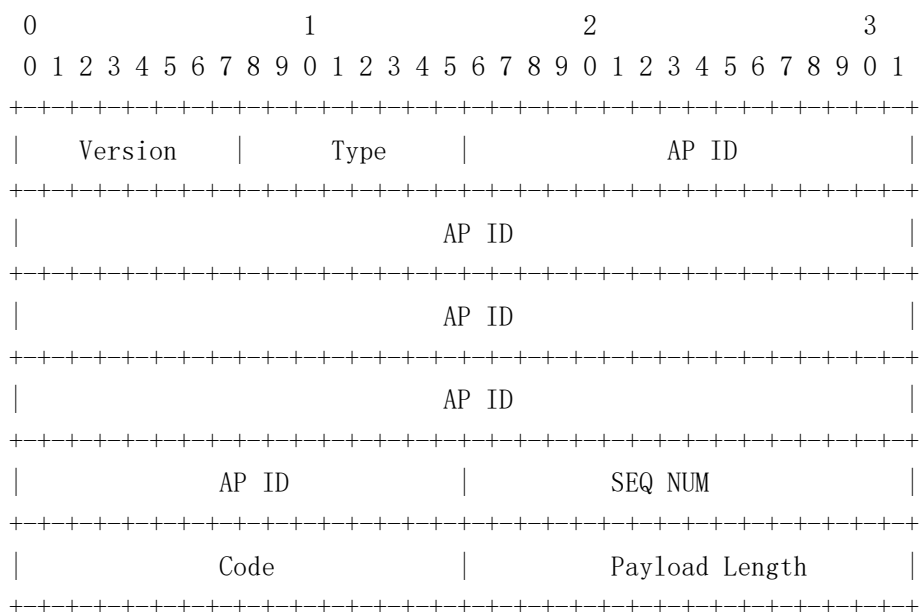
3.3 状态转移图

	INIT (S0)	DISCV (S1)	JOIN (S2)	IMAGE (S3)	RUN (S4)	WAIT (S5)	RECOV (S6)
DISCV REQ(E0)	A0/S1						
DSCV REP(E1)		A1/S2					
JOIN REQ NO UPDATE(E2)			A2/S4				
JOIN REQ UPDATE(E3)			A3/S3				
JOIN TIMER(E4)			A4/S0				
UPDATE DONE(E5)				A5/S0			
ECHO REQ(E6)					A6/S4		
ECHO TIMER(E7)					A7/S5		
RECONN REQ(E8)						A8/S6	
WAIT TIMER(E9)						A9/S0	
RECOV OK(E10)							A10/S4
RECOV ERROR(E11)							A11/S0

四、协议基本格式

4.1 协议头

协议头如下图所示



Version：表示协议版本。

Type：表示数据加密模式，

0 - 表示不加密

1 - 表示加密协商阶段

2 - 表示加密通信阶段

AP ID：AP 的身份唯一标识符，长度最大为 16 字节，长度不够以 0 填充，可以采用 AP 的 MAC 地址或者 UUID，建议采用 UUID

SEQ NUM：表示消息的序号，由 AP 产生，AP 忽略 SEQ NUM 不正确的消息。

Code：消息类型

1-1024 本协议使用

其他值为厂商自由扩展使用

Payload Length : 有效消息长度。

4.2 协议具体格式定义

4.2.1 密钥请求 (Secret Key Request)

Code : 1

Secret Key Request 报文由 AP 发给 AC , 必须携带如下消息元素

AP Secret Key

4.2.2 密钥回复 (Secret Key Response)

Code : 2

Secret Key Response 报文由 AC 发给 AP , 必须携带如下消息元素

Result Code

4.2.3 发现请求 (Discover Request)

Code : 3

Discovery Request 报文由 AP 发给 AC , 必须携带如下消息元素

AP Board Data

4.2.4 发现回应 (Discover Response)

Code : 4

Discover Response 报文由 AC 发给 AP，必须携带如下消息元素

AC IPv4 Address

4.2.5 加入请求 (Join Request)

Code : 5

Join Request 报文由 AP 发给 AC，必须携带如下消息元素

AP Board Data

4.2.6 加入回应 (Join Response)

Code : 6

Join Response 报文由 AC 发给 AP，必须携带如下消息元素

Result Code

可能包含以下消息元素

Echo Time

Idle Time

WIFI Configuration

Portal Configuration

Image Identifier

4.2.7 回声请求 (Echo Request)

Code : 7

Echo Request 报文由 AP 发给 AC，不包含任何消息

4.2.8 回声响应 (Echo Response)

Code : 8

Echo Response 报文由 AC 发给 AP , 不包含任何消息

4.2.9 重启 AP 请求 (Reboot Request)

Code : 9

Reboot Request 由 AC 发给 AP , 该消息不包含任何消息

4.2.10 重启 AP 回复 (Reboot Response)

Code : 10

Reboot Response 由 AP 发给 AC , 该消息不包含任何消息

4.2.11 AP 重连请求 (Reconnect Request)

Code : 11

Reconnect Request 由 AP 发给 AC , 该消息不包含任何消息

4.2.12 AP 重连回复 (Reconnect Response)

Code : 12

Reconnect Response 由 AC 发给 AP , 该消息必须包含如下消息

Result Code

4.2.13 AP 恢复会话请求 (Recover Request)

Code : 13

Recover Request 由 AP 发给 AC , 该消息可能包含如下消息

Echo Time

Idle Time

WIFI Configuration

Portal Configuration

User Statistics

4.2.14 AP 恢复会话回复 (Recover Response)

Code : 14

Recover Response 由 AC 发给 AP , 该消息必须包含如下信息

Result Code

4.2.15 固件完成 (Image Data Response)

Code : 16

Image Data Response 由 AP 发给 AC , 该消息必须包含如下消息

Result Code

4.2.16 新用户请求 (New User Request)

Code : 50

New User Request 由 AP 发给 AC , 该消息必须包含以下消息

User Information

4.2.17 新用户回复 (New User Response)

Code : 51

New User Response 由 AC 发给 AP , 该消息必须包含以下消息

User Information

4.2.18 用户授权请求 (User Accredit Request)

Code : 52

User Accredit Request 由 AC 发给 AP , 该消息必须包含以下消息

User Quota

4.2.19 用户授权回复 (User Accredit Response)

Code : 53

User Accredit Response 由 AP 发给 AC , 该消息必须包含以下消息

User Information

4.2.20 用户下线请求 (User Left Request)

Code : 54

User Left Request 由 AP 发给 AC , 该消息必须包含以下消息

User Statistics

4.2.21 用户下线回复 (User Left Response)

Code : 55

User Left Response 由 AC 发给 AP , 该消息必须包含以下消息

User Information

4.2.22 强制用户下线请求 (User Drop Request)

Code : 56

User Drop Request 由 AC 发给 AP , 该消息必须包含以下消息

User Information

4.2.23 强制用户下线回复 (User Drop Response)

Code : 57

User Drop Response 由 AP 发给 AC , 该消息必须包含以下消息

User Statistics

4.2.24 用户计费请求 (User Account Request)

Code : 58

User Account Request 由 AP 发给 AC , 该消息必须包含以下消息一个或多个

个

User Statistics

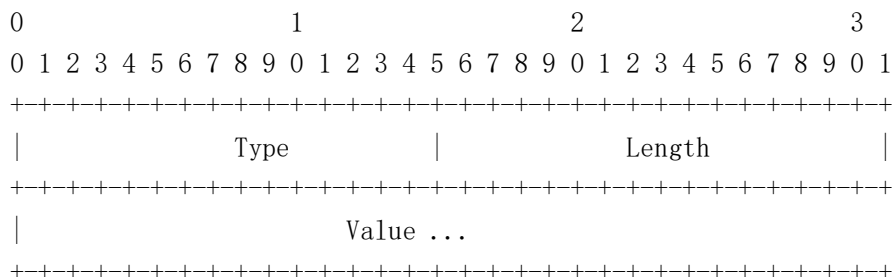
4.2.25 用户计费回复 (User Account Response)

Code : 59

User Account Response 由 AP 发给 AC , 该消息不包含任何消息

五、消息属性

消息属性采用 TLV 的格式封装



Type : 消息类型

1 - 1024 本协议保留使用

其他值供扩展

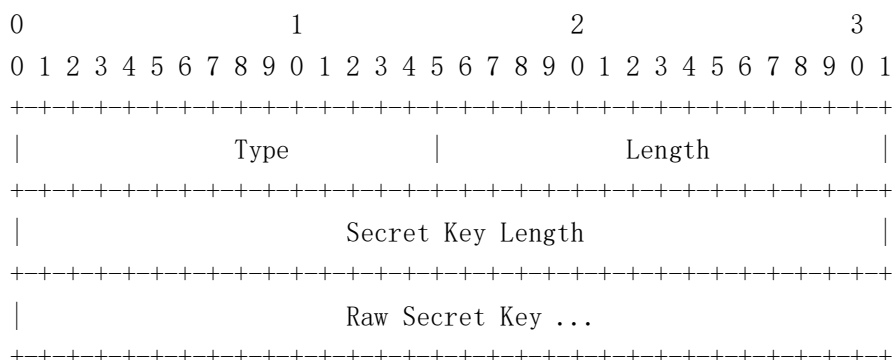
Length : 消息长度, 不包括 Type 与 Length 的长度, 仅仅表示 Value 的

长度, length 长度不能超过 512 字节

Value : 有效消息内容

5.1 Secret Key

Secret Key 为 AP 产生的 AES 密钥



Type : 1

Length : >5

Secret Key Length : AES 扩展密钥长度

Raw Secret Key : AP 随机产生的原始 AES 密钥, 最大长度不超过 64 字节

5.2 AP Board Data

1										2										3												
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	
+-----+																																

Type : 2

Length : >4

Major Version : AP 固件主版本

Minor Version : AP 固件子版本

Hardware : AP 硬件型号字符串, 最大长度不超过 64 字节

5.3 AC IPv4 地址 (AC IPv4 Address)

0	1										2										3										
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
+ +																															

Type : 3

Length : >4

Ipv4 : AC 的 IPv4 地址

5.4 Result Code

0	1									2									3													
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	
+-----																																

Type : 4

Length : 4

Code : 结果值 ,

0 – 成功

1 – 失败

2 – 错误

5.5 Echo Time

Echo Time 为 AP 与 AC 之间的心跳保活时间

0	1									2									3													
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	
+ +																																

Type : 5

Length : 4

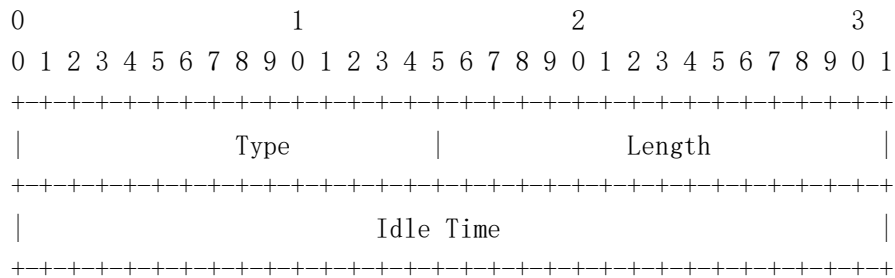
Echo Time : 大于零的正整数。单位秒 , 如果 AC 为云部署 , 该值请注意

设置大小不能超过网络 NAT 阈值

5.6 Idle Time

Idle Time 为用户之间保活时间，用户在此时间内无流量产生即视为已下线

离开

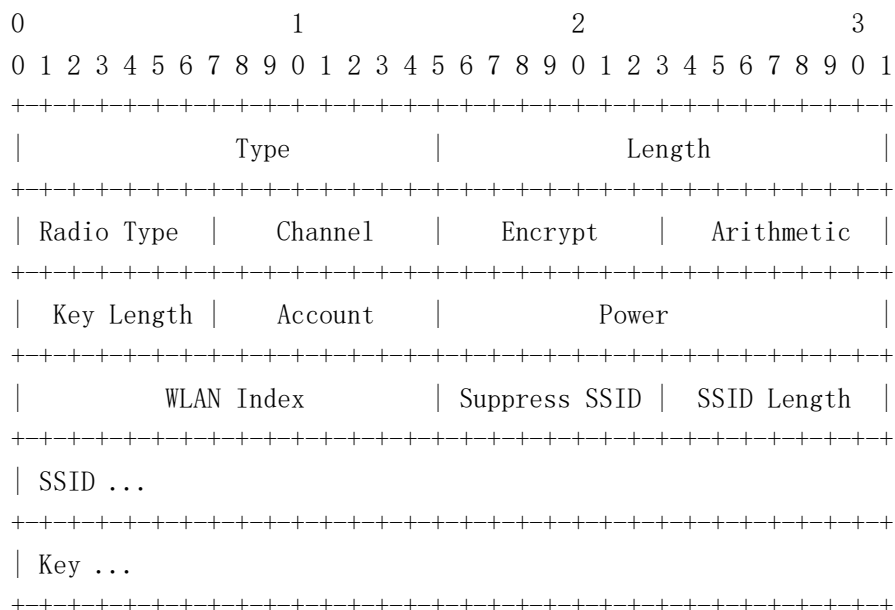


Type : 6

Length : 4

Idle Time : 大于零的正整数。单位秒

5.7 WiFi Configuration



Type : 7

Length : >12

Radio Type : 802.11 无线类型, 正整数, 具体值见附录 802.11 无线类型代码定义

Channel : 无线频道, 正整数, 请遵守无线相关法规与无线信号的干扰进行设置

Encrypt : 无线加密方式, 为 0 表示开启 Portal 认证方式, 其他值参考附录 7.3 无线加密代码定义

Arithmetic : 无线加密算法, 当 Encrypt 等于时, 该值无效。其值参考附录 7.4 无线加密算法代码定义

Key Length : 无线密码长度

Account : 该 SSID 是否开启计费功能

Power : 无线发射功率, 单位毫瓦 (mW)

WLAN Index : 无线的虚拟网络接口序号, 从 0 开始, 为 0 表示 wlan0 , 其他依次类推

Suppress SSID : 是否隐藏 SSID

0 – 不隐藏

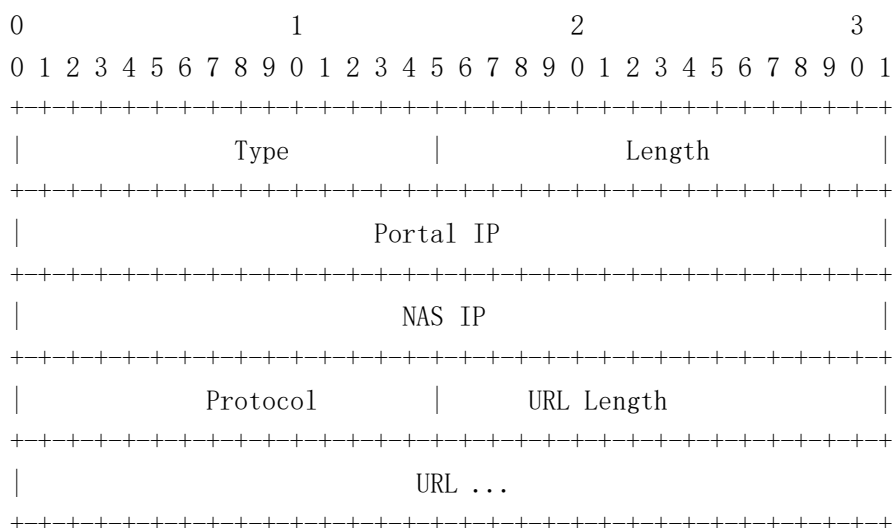
1 – 隐藏

SSID Length : SSID 长度

SSID : 无线名称, 字符串, 长度不能超过 32 字节

Key : 无线密码内容, 字符串

5.8 Portal Configuration



Type : 8

Length : >8

Protocol : Portal 的协议码，具体值见附录 7.2 节《Portal 协议代码定义》

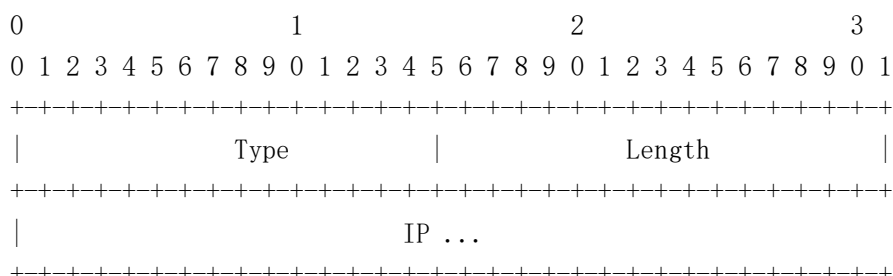
Portal IP : Portal 服务器 IPv4 地址

NAS IP : 与 portal 对接的 NAS 地址

URL Length : Portal URL 的长度，不能超过 253 字节

URL : Portal URL 字符串，必须以 http://或者 https://开头

5.9 Free IP



Type : 9

Length : ≥ 4

IP : IPv4 的值

5.10 Image Identifier

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			
+++++	+++++	+++++	+++++
	Type		Length
+++++	+++++	+++++	+++++
	File Size		
+++++	+++++	+++++	+++++
	Image MD5		
+++++	+++++	+++++	+++++
	Image MD5		
+++++	+++++	+++++	+++++
	Image MD5		
+++++	+++++	+++++	+++++
	Image MD5		
+++++	+++++	+++++	+++++
	Image Name ...		
+++++	+++++	+++++	+++++

Type : 10

Length : > 20

File Size : AP 固件文件大小, 单位字节

Image MD5 : AP 固件 MD5 值, 二进制数据, 长度为 16 字节

Image Name : AP 固件名字, 字符串, 长度不超过 64 字节

5.11 Account Time

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			
+++++	+++++	+++++	+++++
	Type		Length
+++++	+++++	+++++	+++++

```
| Account Time |
|-----|
```

Type : 11

Length : 4

Account Time : 计费统计上报时间周期, 单位秒, 如果为 0, 则表示不上报。

5.12 Free Host

```

0           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
|-----|
|           Type           |           Length           |
|-----|
|           Host...        |
|-----|

```

Type : 12

Length : >1

Host : WWW 主机名字, 字符串, 长度不超过 128 字节。

5.13 User Information

```

0           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
|-----|
|           Type           |           Length           |
|-----|
|           SN             |
|-----|
|           V4IP           |
|-----|
|           MAC            |
|-----|
|           MAC            |           WLAN Index        |
|-----|

```

Error Code

Type : 50

Length : 20

SN : AP 给用户产生的 32 位随机码，主要用于认证

V4IP : 用户的 IP 地址

MAC : 用户的 MAC 地址

WLAN Index : 用户接入的无线序号，其值参考 WiFi Configuration

Error Code : 在请求消息中无效，在回复消息中，其值参考 Result Code

5.14 User Quota

0	1	2	3																
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1																			
Type										Length									
SN																			
V4IP																			
MAC																			
MAC										WLAN Index									
Session Time																			
In Speed																			
Out Speed																			

Type : 51

Length : 28 字节

SN : AP 给用户产生的 32 位随机码，主要用于认证

V4IP : 用户的 IP 地址

MAC : 用户的 MAC 地址

WLAN Index : 用户接入的无线序号，其值参考 WiFi Configuration

Session Time : 本次用户上网时长限制，单位秒，0 为无限制

In Speed : 用户的下行速度，单位为字节每秒(B/S)，0 为无限制

Out Speed : 用户的上行速度，单位为字节每秒(B/S)，0 为无限制

5.15 User Statistics

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			
+	+	+	+
	Type		Length
+	+	+	+
	V4IP		
+	+	+	+
	MAC		
+	+	+	+
	MAC		Error Code
+	+	+	+
	Online Time		
+	+	+	+
	In Giga-Bytes		
+	+	+	+
	In Bytes		
+	+	+	+
	Out Giga-Bytes		
+	+	+	+
	Out Bytes		
+	+	+	+

Type : 52

Length : 32 字节

V4IP : 用户的 IP 地址

MAC : 用户的 MAC 地址

Error Code : 错误码, 在计费消息中无效, 在强制下线中

0 – OK

1 – 用户不存在

Online Time : 用户在线时长, 单位秒

In Giga-Bytes : 用户下行流量吉兆(GB)级别计数, 计算流量时该值需要

2^{30} (2 的 30 次方)

In Bytes : 用户下行流量吉兆字节以下计数

Out Giga-Bytes : 用户上行流量吉兆(GB)级别计数, 计算流量时该值需

要 2^{30} (2 的 30 次方)

Out Bytes : 用户上行流量吉兆(GB)字节以下计数

六、AP 固件升级

如果 AP 在 JOIN 回复消息中包含了 Image Identifier 消息属性，则认为有新的固件版本可用。下载 AP 固件采用 HTTP 的方式下载，下载好固件后，需要对比文件的 MD5 值，然后再进行升级，升级结果上报 AC，最后重启 AP。

七、消息加密

消息加密采用 AES 方式，由于 AP 资源有限，建议扩展密钥使用 128 位。

密钥协商阶段参考 https 的密钥协商方法。

- (1) AP 通过 http 的方式获取 AC 的 RSA 的公钥
- (2) AP 通过 RSA 公钥加密 AES 密钥请求消息，向 AC 发起密钥请求
- (3) AC 使用 RSA 私钥解密 AP 的密钥请求消息，AC 使用该 AES 密钥加密
密钥请求回复消息，通知 AP 是否使用该 AES 密钥
- (4) 如果确定使用该密钥，则 AP 与 AC 后续通信使用该密钥加密

八、附录

8.1 802.11 无线类型代码定义

无线类型代码	802.11 无线类型
1	802.11
2	802.11a
3	802.11b
4	802.11c
5	802.11d
6	802.11e
7	802.11f
8	802.11g
9	802.11h
10	802.11i
11	802.11j
12	802.11k
13	802.11l
14	802.11m
15	802.11n
16	802.11o
17	802.11p
18	802.11q
19	802.11r
20	802.11s
21	802.11t
22	802.11u
23	802.11v
24	802.11ac
25	802.11ad
26	802.11ae

8.2 Portal 协议代码定义

Portal 协议代码	Portal 协议	备注
1	华为 Portal 协议	华为公司的 Portal 协议，主要对接其交换机
2	CMCC Portal 协议	中国移动推出的 WLAN 业务 Portal 协议

3	NatShell Portal 协议	蓝海卓越
---	--------------------	------

8.3 无线加密代码定义

无线加密代码	加密方式	备注
1	WPA	Wi-Fi Protected Access - Wi-Fi 网络安全接入
2	WPA-PSK	WPA 预先共享密钥
3	WPA2	WPA 第二版
4	WPA2-PSK	WPA2 预先共享密钥

8.4 无线加密算法代码定义

加密算法代码	加密算法	备注
0	自动	AP 自动选择
1	TKIP	临时密钥完整性协议
2	AES	高级加密算法